

IQI 04, Seminar 8

Produced with pdflatex and xfig

- Implementing the Toffoli gate.
- Multi-controlled gates.
- Universality.

E. "Manny" Knill: knill@boulder.nist.gov

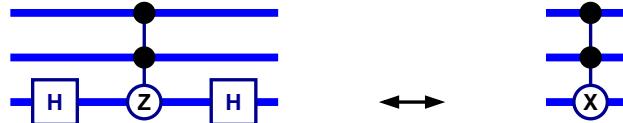


TOC

Controlled Sign Flips

- Controlled sign flips \leftrightarrow controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



- Exponential forms for sgn, csgn, c²sng.

$$\text{sgn} = \sigma_z = e^{-\frac{i}{2}(1-Z)\pi}$$

$$\text{csgn}^{(AB)} = \exp(i(|1\rangle_A^A\langle 1|)(|1\rangle_B^B\langle 1|)\pi)$$

$$= e^{\frac{i}{4}(1-Z^{(A)})(1-Z^{(B)})\pi}$$

$$\text{c}^2\text{sgn}^{(ABC)} = \exp(i(|1\rangle_A^A\langle 1|)(|1\rangle_B^B\langle 1|)(|1\rangle_C^C\langle 1|)\pi)$$

$$= e^{\frac{i}{4}(1-Z^{(A)})(1-Z^{(B)})(1-Z^{(C)})\pi}$$

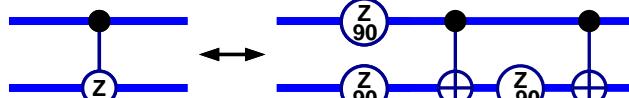


1
TOC

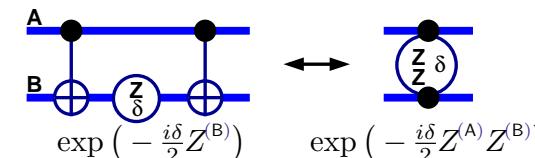
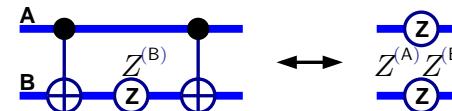
Controlled Sign Flip Implementations

- Decomposition of csgn.

$$\text{csgn}^{(AB)} = e^{\frac{i\pi}{4}(1-Z^{(A)})(1-Z^{(B)})} = e^{\frac{i\pi}{4}} e^{-\frac{i\pi}{4}Z^{(A)}} e^{-\frac{i\pi}{4}Z^{(B)}} e^{\frac{i\pi}{4}Z^{(A)}Z^{(B)}}$$



- Recall conjugation rules.

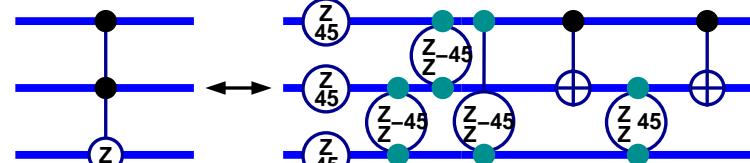


2
TOC

Controlled Sign Flip Implementations

- Decomposition of c²sng.

$$\begin{aligned} \text{c}^2\text{sgn}^{(ABC)} &= e^{\frac{i\pi}{8}(1-Z^{(A)})(1-Z^{(B)})(1-Z^{(C)})} \\ &= e^{\frac{i\pi}{8}} e^{-\frac{i\pi}{8}Z^{(A)}} e^{-\frac{i\pi}{8}Z^{(B)}} e^{-\frac{i\pi}{8}Z^{(C)}} \\ &\quad e^{\frac{i\pi}{8}Z^{(A)}Z^{(B)}} e^{\frac{i\pi}{8}Z^{(A)}Z^{(C)}} e^{\frac{i\pi}{8}Z^{(B)}Z^{(C)}} e^{-\frac{i\pi}{8}Z^{(A)}Z^{(B)}Z^{(C)}} \end{aligned}$$

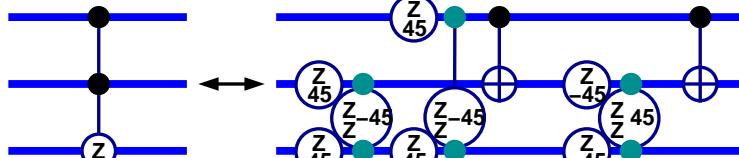


3
TOC

Controlled Sign Flip Implementations

- Decomposition of $c^2 \text{sgn}$.

$$\begin{aligned} c^2 \text{sgn}^{(ABC)} &= e^{\frac{i\pi}{8}} (1 - Z^{(A)}) (1 - Z^{(B)}) (1 - Z^{(C)}) \\ &= e^{\frac{i\pi}{8}} \mathbb{1} e^{-\frac{i\pi}{8} Z^{(A)}} e^{-\frac{i\pi}{8} Z^{(B)}} e^{-\frac{i\pi}{8} Z^{(C)}} \\ &\quad e^{\frac{i\pi}{8} Z^{(A)} Z^{(B)}} e^{\frac{i\pi}{8} Z^{(A)} Z^{(C)}} e^{\frac{i\pi}{8} Z^{(B)} Z^{(C)}} e^{-\frac{i\pi}{8} Z^{(A)} Z^{(B)} Z^{(C)}} \end{aligned}$$



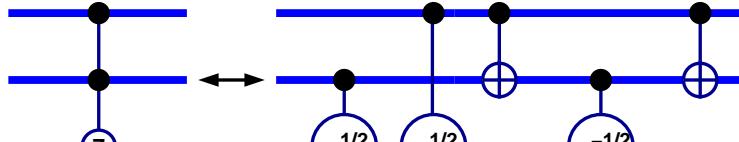
4

TOC

Controlled Sign Flip Implementations

- Decomposition of $c^2 \text{sgn}$.

$$\begin{aligned} c^2 \text{sgn}^{(ABC)} &= e^{\frac{i\pi}{8}} (1 - Z^{(A)}) (1 - Z^{(B)}) (1 - Z^{(C)}) \\ &= e^{\frac{i\pi}{8}} \mathbb{1} e^{-\frac{i\pi}{8} Z^{(A)}} e^{-\frac{i\pi}{8} Z^{(B)}} e^{-\frac{i\pi}{8} Z^{(C)}} \\ &\quad e^{\frac{i\pi}{8} Z^{(A)} Z^{(B)}} e^{\frac{i\pi}{8} Z^{(A)} Z^{(C)}} e^{\frac{i\pi}{8} Z^{(B)} Z^{(C)}} e^{-\frac{i\pi}{8} Z^{(A)} Z^{(B)} Z^{(C)}} \end{aligned}$$



Examine:

$$\begin{aligned} A & \left(\begin{array}{c} Z_{45} \\ Z_{-45} \end{array} \right) \leftrightarrow \left(\begin{array}{c} z^{1/2} \end{array} \right) \\ B & \left(\begin{array}{c} Z_{45} \\ Z_{-45} \end{array} \right) \leftrightarrow \left(\begin{array}{c} z^{1/2} \end{array} \right) \end{aligned}$$

$$\exp \left(-\frac{i\pi}{8} Z^{(A)} - \frac{i\pi}{8} Z^{(B)} + \frac{i\pi}{8} Z^{(A)} Z^{(B)} \right)$$

$$= \exp \left(-\frac{i\pi}{8} \right) \exp \left(\frac{i\pi}{8} (\mathbb{1} - Z^{(A)}) (\mathbb{1} - Z^{(B)}) \right)$$

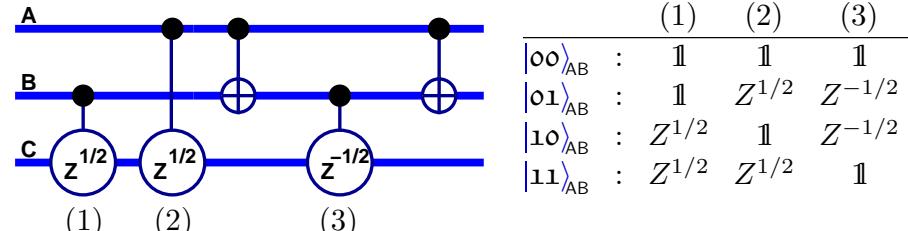
$$\propto |\alpha_A^A\rangle\langle\alpha| - |\alpha_A^A\rangle\langle\alpha|(|\alpha_B^B\rangle\langle\alpha| + i|\alpha_B^B\rangle\langle\alpha|)$$

5

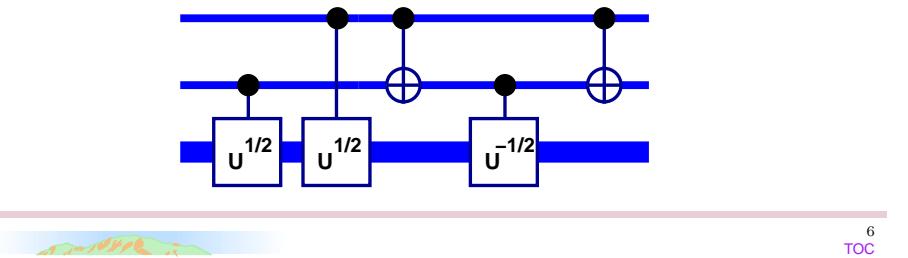
TOC

Controlled² Unitary

- Generalizing the controlled² Z implementation.



- Same for a unitary U with controlled- $U^{\pm 1/2}$ implementations.



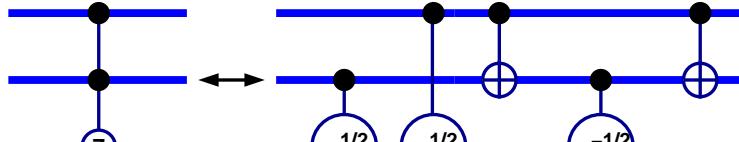
6

TOC

Controlled Sign Flip Implementations

- Decomposition of $c^2 \text{sgn}$.

$$\begin{aligned} c^2 \text{sgn}^{(ABC)} &= e^{\frac{i\pi}{8}} (1 - Z^{(A)}) (1 - Z^{(B)}) (1 - Z^{(C)}) \\ &= e^{\frac{i\pi}{8}} \mathbb{1} e^{-\frac{i\pi}{8} Z^{(A)}} e^{-\frac{i\pi}{8} Z^{(B)}} e^{-\frac{i\pi}{8} Z^{(C)}} \\ &\quad e^{\frac{i\pi}{8} Z^{(A)} Z^{(B)}} e^{\frac{i\pi}{8} Z^{(A)} Z^{(C)}} e^{\frac{i\pi}{8} Z^{(B)} Z^{(C)}} e^{-\frac{i\pi}{8} Z^{(A)} Z^{(B)} Z^{(C)}} \end{aligned}$$



Examine:

$$\begin{aligned} A & \left(\begin{array}{c} Z_{45} \\ Z_{-45} \end{array} \right) \leftrightarrow \left(\begin{array}{c} z^{1/2} \end{array} \right) \\ B & \left(\begin{array}{c} Z_{45} \\ Z_{-45} \end{array} \right) \leftrightarrow \left(\begin{array}{c} z^{1/2} \end{array} \right) \end{aligned}$$

$$\exp \left(-\frac{i\pi}{8} Z^{(A)} - \frac{i\pi}{8} Z^{(B)} + \frac{i\pi}{8} Z^{(A)} Z^{(B)} \right)$$

$$= \exp \left(-\frac{i\pi}{8} \right) \exp \left(\frac{i\pi}{8} (\mathbb{1} - Z^{(A)}) (\mathbb{1} - Z^{(B)}) \right)$$

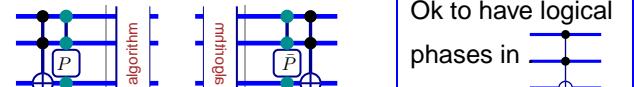
$$\propto |\alpha_A^A\rangle\langle\alpha| - |\alpha_A^A\rangle\langle\alpha|(|\alpha_B^B\rangle\langle\alpha| + i|\alpha_B^B\rangle\langle\alpha|)$$

5

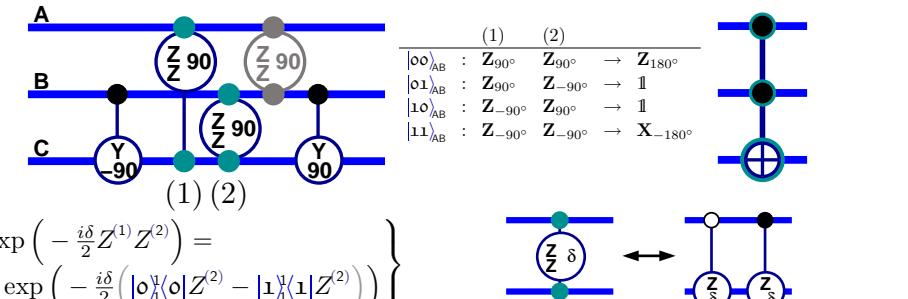
TOC

Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



- Consider $e^{-\frac{i\pi}{8} Z^{(A)} Z^{(C)}} e^{-\frac{i\pi}{8} Z^{(B)} Z^{(C)}}$ as AB-controlled:

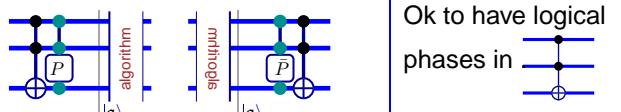


7

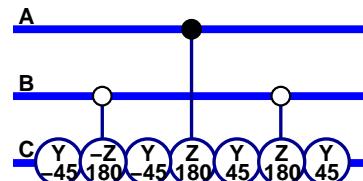
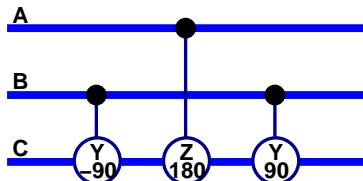
TOC

Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



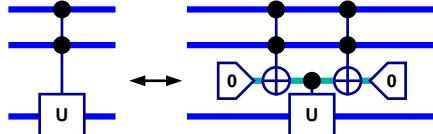
- Two more Toffolis up to logical phases.



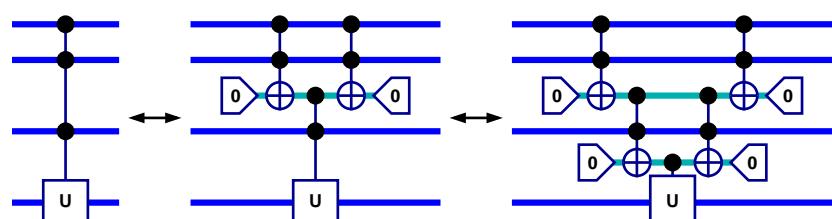
8
TOC

Adding Controls

- Add a control using an ancilla and two $c^2\text{not}$ gates.



- Add multiple controls.

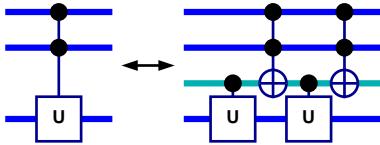


- n controls: $2(n - 1)$ $c^2\text{not}$, $n - 1$ ancillas, 1 cU gates.

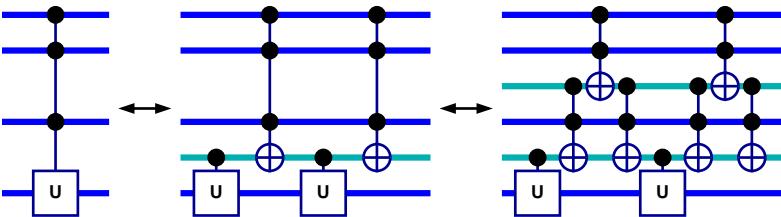
9
TOC

Adding Controls without Prepared Ancillas

- Suppose that $U^2 = \mathbb{1}$.



- Add multiple controls without prepared ancillas.

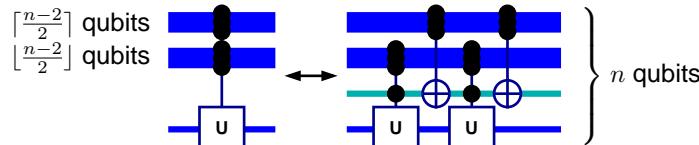


- n controls: $4(n - 3) + 2$ $c^2\text{not}$, $2n$ qubits, 2 cU gates.

10
TOC

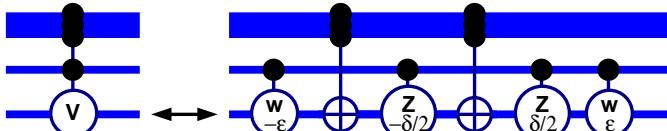
Controlled U With 0 or 1 Extra Qubit

- Halving controls for $U^2 = \mathbb{1}$, n controls.



- $n - 2$ controls: $8(n - 5)$ $c^2\text{not}$, n qubits, 2 cU , 2 cnot .

- Let V be a rotation. With appropriate choice of parameters:

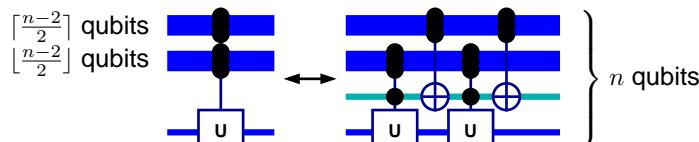


- $n - 1$ controls: $16(n - 5)$ $c^2\text{not}$, 8 cnot , n qubits, 4 cRot .

11
TOC

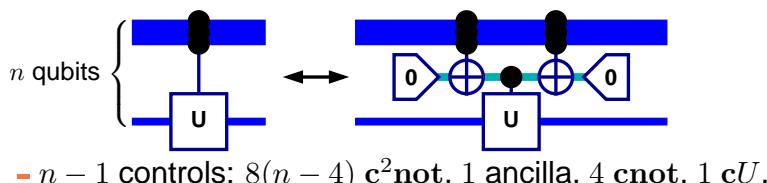
Controlled U With 0 or 1 Extra Qubit

- Halving controls for $U^2 = \mathbb{1}$, n controls.



- $n - 2$ controls: $8(n - 5)$ $c^2\text{not}$, n qubits, 2 cU , 2 cnot .

- Let U be arbitrary. From before:



Time/space tradeoff?

Barenco et al 1995 [1]

12
TOC

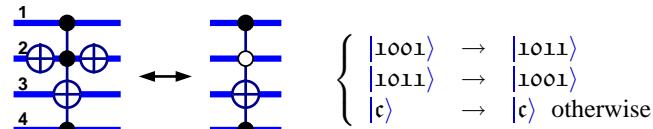
Universality: Permutations of Logical States

- $c^k\text{not}$ gates implement all logical state permutations.

Proof. Consider n qubits.

- If $|\alpha - \beta| = 1$, the transposition $|\alpha\rangle \leftrightarrow |\beta\rangle$ is implementable.

Example: $\alpha = 1001$ and $\beta = 1011$:

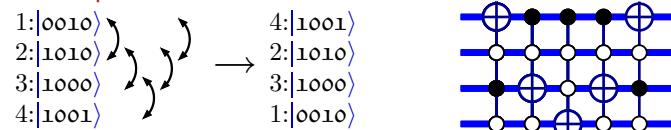


- β can be reached from α by a sequence changing one bit at a time.

Example: $\alpha = 0010$ and $\beta = 1001$: $0010 \leftrightarrow 1010 \leftrightarrow 1000 \leftrightarrow 1001$

- Every transposition $|\alpha\rangle \leftrightarrow |\beta\rangle$ is implementable.

Example: $\alpha = 0010$ and $\beta = 1001$:



- Every permutation is a product of transpositions.

13
TOC

Universality: Unitary Operators

- Controlled^k one-qubit gates implement all unitary operators.

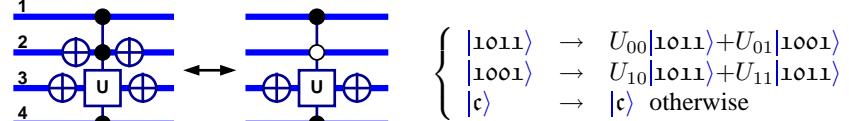
Proof. Consider n qubits.

For a one-qubit unitary U , define the “Givens rotation” $G(U, \alpha, \beta)$ by

$$|\alpha\rangle \rightarrow U_{00}|\alpha\rangle + U_{10}|\beta\rangle, |\beta\rangle \rightarrow U_{01}|\alpha\rangle + U_{11}|\beta\rangle \text{ and } |\gamma\rangle \rightarrow |\gamma\rangle \text{ (otherwise).}$$

- If $|\alpha - \beta| = 1$ then $G(U, \alpha, \beta)$ is implementable.

Example: $\alpha = 1011$ and $\beta = 1001$:



- Let P be a permutation that maps $\alpha \rightarrow \alpha'$ and $\beta \rightarrow \beta'$.

Then $G(U, \alpha', \beta') = PG(U, \alpha, \beta)P^\dagger$.

$$\left| \begin{array}{l} \alpha' \\ \beta' \end{array} \right\rangle \xrightarrow{P^\dagger} \left| \begin{array}{l} \alpha \\ \beta \end{array} \right\rangle \xrightarrow{G(U, \alpha, \beta)} \left\{ \begin{array}{l} U_{00}|\alpha\rangle + U_{10}|\beta\rangle \\ U_{01}|\alpha\rangle + U_{11}|\beta\rangle \end{array} \right\} \xrightarrow{P} \left| \begin{array}{l} U_{00}|\alpha'\rangle + U_{10}|\beta'\rangle \\ U_{01}|\alpha'\rangle + U_{11}|\beta'\rangle \end{array} \right\rangle$$

- Every Givens rotation is implementable.

- Every unitary operator is a product of Givens rotations.

14
TOC

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$\left(\begin{array}{cccc} G_{34} & G_{24} & G_{23} & \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0.8 & 0.6 \\ 0 & 0 & 0.6 & 0.8 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -0.8 & 0 & 0.6 \\ 0 & 0 & 1 & 0 \\ 0 & 0.6 & 0.8 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0.8 & -0.6 & 0 \\ 0 & 0.6 & 0.8 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} & \times \end{array} \right)$$

$$\left(\begin{array}{cccc} G_{14} & G_{13} & G_{12} & M \\ \begin{pmatrix} .8 & 0 & 0 & 0.6 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -0.8 \end{pmatrix} & \begin{pmatrix} .6 & 0 & 0.8 & 0 \\ 0 & 1 & 0 & 0 \\ -0.8 & 0 & 0.6 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} .8 & 0 & 0 & 0 \\ -0.6 & 0.8 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix} \end{array} \right)$$

$$M = G_{12}^\dagger G_{13}^\dagger G_{14}^\dagger G_{23}^\dagger G_{24}^\dagger G_{34}^\dagger = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

15
TOC

Universality: Resources

Consider n qubit unitary operators.

- The number of **cnot** and one-qubit gates needed to implement a unitary operator U is

$$O((2^n)^2) = O(4^n)$$

Vartiainen&al 2003 [2]

- There are unitary operators that require $\Omega(4^n)$ **cnot** and one-qubit gates.

Barenco&al 1995 [1]

- Almost all* unitary operators require $2^{\Omega(n)}$ **cnot** and one-qubit gates to approximate U with error $c - \epsilon$, where c is the average distance between unitary operators.

Knill 1995 [3, 4]

*... except for an exponentially small fraction according to the Haar measure.

16
TOC

References

- [1] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, 1995.
- [2] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa. Efficient decomposition of quantum gates. *quant-ph/0312218*, 2003.
- [3] E. Knill. Approximation by quantum circuits. Technical Report LAUR-95-2225, Los Alamos National Laboratory, knill@lanl.gov, 1995. *quant-ph/9508006*.
- [4] E. Knill. Bounds for approximation in total variation distance by quantum circuits. Technical Report LAUR-95-2724, Los Alamos National Laboratory, 1995. *quant-ph/9508007*.

18
TOC

Contents

Title: IQI 04, Seminar 8.....	0	Adding Controls without Prepared Ancillas	10
Controlled Sign Flips	1	Controlled U With 0 or 1 Extra Qubit I	11
Controlled Sign Flip Implementations I	2	Controlled U With 0 or 1 Extra Qubit II	12
Controlled Sign Flip Implementations II	3	Universality: Permutations of Logical States	13
Controlled Sign Flip Implementations III	4	Universality: Unitary Operators	14
Controlled Sign Flip Implementations IV	5	Givens Rotation Decomposition	15
Controlled ² Unitary	6	Universality: Resources	16
Toffoli Gate up to Control Phases I	7	References	18
Toffoli Gate up to Control Phases II	8		
Adding Controls	9		

17
TOC